CIBER E-DEA

Boletín de Seguridad

123456 sigue siendo la contraseña más usada en 2025: ¿qué riesgo representa?

Incidentes de Ciberseguridad en el 2025

Análisis de Tendencias y Prioridades Tecnológicas 2026

PANORAMA DE RIESGOS EN EL 2026

Vulnerabilidades destacadas

Ciber Incidentes en Colombia y en el mundo

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada NOV 2024 - NOV 2025 COL
icontec ISO 9001 CO-SC-CER890596
icontec ISO 45001 CO-ST-CER890599
icontec ISO / IEC 27001 CO-SI-2001607
IQNET CERTIFIED MANAGEMENT SYSTEM

123456 sigue siendo la contraseña más usada en 2025: ¿qué riesgo representa?

A pesar del avance en tecnologías de seguridad y del aumento de incidentes de ciberseguridad, las contraseñas débiles siguen siendo uno de los principales puntos de entrada para los atacantes. En 2025, la contraseña más utilizada a nivel global continúa siendo “123456”, una combinación trivial que puede ser vulnerada en segundos mediante ataques automatizados. Este comportamiento confirma que el problema no es tecnológico, sino cultural y operativo.

Las contraseñas más usadas en 2025
(Basado en análisis de bases de datos de credenciales filtradas y estudios de seguridad)

(“123456” lidera ampliamente frente al resto de combinaciones)

Se evidencia que una pequeña cantidad de contraseñas extremadamente simples concentra un alto porcentaje de uso, facilitando ataques de fuerza bruta y credential stuffing sin necesidad de técnicas avanzadas.

Un hábito que afecta a todos

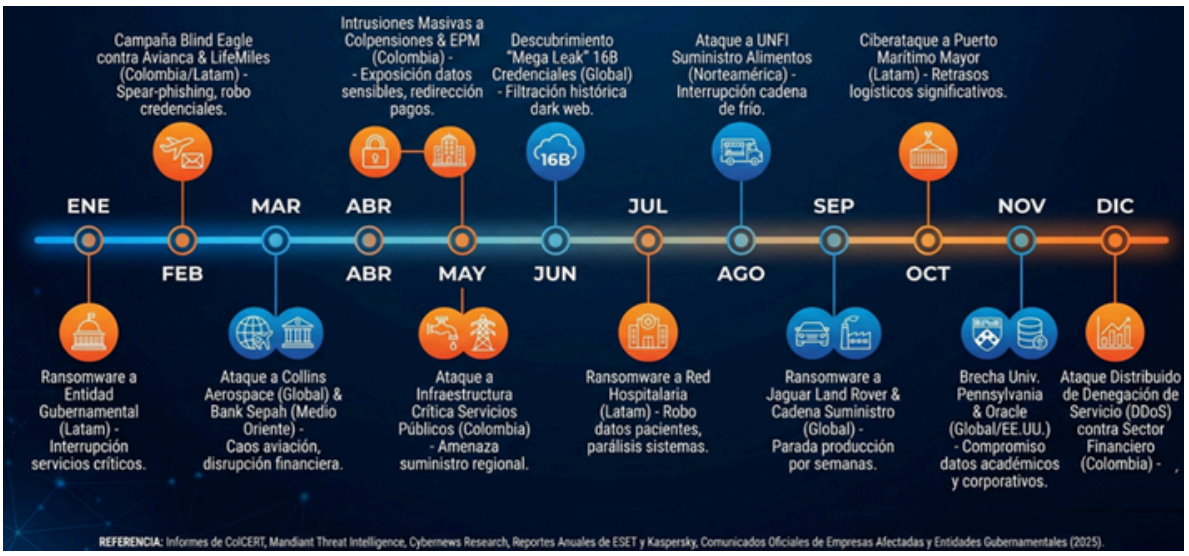
El uso de contraseñas débiles no distingue edad ni nivel técnico. Estudios recientes muestran que estas prácticas se repiten en usuarios jóvenes, perfiles profesionales y entornos corporativos, impulsadas por la comodidad y la reutilización de credenciales.

En Latinoamérica, países como Colombia, México, Brasil y Chile presentan patrones similares, lo que incrementa el riesgo tanto a nivel personal como organizacional.

Más Información

Incidentes de Ciberseguridad en el 2025

Con la consolidación de la IA ofensiva y ataques cada vez más dirigidos a la infraestructura crítica, tanto el mundo como Colombia enfrentaron desafíos sin precedentes.



Lecciones Vitales tras los Incidentes de 2025
El 2025 nos enseñó que la ciberseguridad ya no es un "problema de sistemas", sino un pilar de la continuidad del negocio.

La Identidad es el Nuevo Perímetro
Los ataques a Salesforce y el robo de tokens OAuth demostraron que las contraseñas ya no son suficientes. No basta con tener MFA (Autenticación de Múltiples Factores); es necesario migrar a esquemas de autenticación resistente al phishing (como llaves de seguridad físicas) y monitorear el secuestro de sesiones en tiempo real. Si el atacante roba el "token" de acceso, entrará sin necesidad de contraseña.

Gestión Estricta de Riesgos de Terceros (TPRM)
Casos como Ingram Micro y el chatbot de McDonald's dejaron claro que somos tan fuertes como nuestro proveedor más débil.
Las empresas deben realizar auditorías técnicas recurrentes a sus proveedores de software y servicios de IA. No se debe delegar la seguridad a ciegas; es imperativo exigir certificaciones de protección de datos y tener un Plan B de contingencia si un proveedor clave queda fuera de línea.

IA para Combatir la IA
El grupo Blind Eagle en Colombia utilizó IA para crear correos de phishing perfectos y difíciles de detectar por el ojo humano.

La defensa debe estar a la altura. Es vital integrar herramientas de IA defensiva que analicen patrones de lenguaje y metadatos de correos electrónicos para bloquear amenazas antes de que lleguen a la bandeja de entrada. La capacitación de empleados debe pasar de "no hagas clic" a simulaciones de ataques dinámicos generados por IA.

Más Información

Análisis de Tendencias y Prioridades Tecnológicas 2026

Para 2026, la innovación estará liderada por la Inteligencia Artificial, pero este avance vendrá acompañado de ciberamenazas más complejas. Según la encuesta global de ISACA, las organizaciones enfrentan el desafío de adoptar tecnologías disruptivas en un entorno marcado por la escasez de profesionales cualificados.
Tendencias Críticas.

1. **Predominio de la IA:** La IA y el aprendizaje automático son la prioridad para el 62% de las empresas, enfocándose en la automatización y el análisis predictivo.
2. **Ciberseguridad Sofisticada:** Los ataques de ingeniería social y ransomware se vuelven más efectivos gracias a la personalización que permite la IA.
3. **Crisis de Talento:** Existe una brecha crítica; aunque el 39% de las empresas busca contratar, la falta de candidatos expertos en auditoría y riesgo pone en peligro la seguridad.
4. **Enfoque en la Nube:** La migración y seguridad en la nube siguen siendo fundamentales, enfrentando retos de cumplimiento y protección de datos.

Estrategias de Preparación

- **Gobernanza y Ética:** Es vital establecer marcos de gestión de riesgos para la IA que aseguren la privacidad, la transparencia y eliminen sesgos algorítmicos.
- **Capacitación Especializada:** Ante la falta de personal externo, las empresas deben invertir en el aprendizaje continuo y certificaciones técnicas para su fuerza laboral actual.
- **Modernización Técnica:** Resulta urgente actualizar infraestructuras heredadas y sistemas obsoletos para cerrar brechas de seguridad y prepararse para la computación cuántica.
- **Resiliencia Operativa:** Se requiere fortalecer la continuidad del negocio mediante simulacros frecuentes y planes de respuesta ante crisis multifuncionales.
- **Cumplimiento Proactivo:** Las organizaciones deben alinear sus operaciones con las nuevas normativas y realizar evaluaciones de riesgo de IA de manera inmediata.

Más Información

PANORAMA DE RIESGOS EN EL 2026

Confrontación geoeconómica

El 2026 comenzó de forma agitada con las intervenciones militares, bloqueos económicos y teléfonos rotos en las negociaciones de conflictos actuales con el potencial de afectarnos a todos, estemos cerca o no, de estos conflictos.

Los países más influyentes del mundo

Fuente:https://www.reddit.com/r/MapPorn/comments/1msdsmr/the_most_powerful_and_influential_countries_in/?tl=es-419

La intervención militar en estados sienta un precedente incómodo para muchos en materia del no reconocimiento del derecho internacional, esto podría ser la nueva forma de proceder de otras naciones sobre territorios que son de su interés y que podrían ser objeto de este tipo de intervenciones, así por ejemplo si China decidiera invadir Taiwan tendría un efecto mundial inmediato en el mercado de microchips, un riesgo para el cual el mundo no está preparado para enfrentar. causando una crisis económica global, escasez de productos desde teléfonos hasta automóviles, colapso de empresas tecnológicas, disparos de la inflación y un daño severo a las cadenas de suministro que tardaría años en recuperarse.

De igual forma el restringir el uso de determinados proveedores en nombre de una soberanía tecnología puede aumentar el riesgo de pérdida de resiliencia al concentrar todos los servicios sobre un mismo proveedor como se evidencio el 2025 en el fallo masivo de AWS.

Algunas formas de protegerse contra estos riesgos son la diversificación de la cadena de suministro y proveedores, así como la inversión en planes de continuidad robustos y probados.

fuente:https://www.merca20.com/grafica-del-dia-el-ranking-de-los-mayores-proveedores-de-servicios-en-la-nube-del-mundo/

La desinformación al alcance de la mano.

Otro gran reto es y será la desinformación, el Bigdata no conoce límites cada vez más se recolectan datos de naciones, organizaciones y personas que con frecuencia son objeto de uso poco ético en donde lo que predomina es la generación de dinero a partir de funcionar en una delgada línea entre lo legal y lo ilegal. Estos

El uso de la IA a puesto sobre la mesa un enorme numero de herramientas que facilitan la creación de contenido falso sin la necesidad de tener conocimientos técnicos de herramientas audiovisuales, la cual ha traído una explosión de contenido falso que cada vez es más difícil de identificar, buena parte de este contenido tiene un carácter disruptivo cuya meta es lograr obtener un mayor número de visualizaciones , lo cual ya trae implícito riesgos como los mensajes de odio lo que lleva a crear polarización con consecuencias que en algunos casos extremos han terminado en conflictos armados y genocidios étnicos.

Más Información

Vulnerabilidades destacadas

vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión vulnerable de canal seguro de Netlogon con un controlador de dominio mediante el protocolo remoto de Netlogon (MS-NRPC).

CVE-2020-1472

Microsoft

CVE-2026-21509

Microsoft Office

La confianza en entradas no confiables en una decisión de seguridad en Microsoft Office permite que un atacante no autorizado eluda una característica de seguridad localmente.

Elvanti Endpoint Manager Mobile (EPMM) contiene una vulnerabilidad de inyección de código que podría permitir a los atacantes lograr la ejecución remota de código no autenticado.

CVE-2026-1281

Elvanti

Ciber incidentes en Colombia y en el mundo

Campañas de Malware Persistente

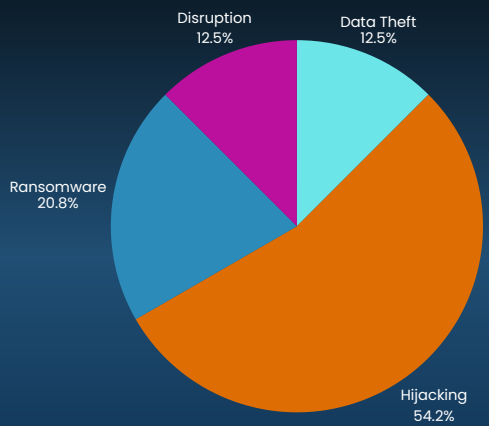
Durante el periodo analizado se presenta un cambio en la dinámica de las detecciones, con cuatro familias registrando incrementos y una reconfiguración clara del panorama observado la semana anterior. **Tycoon 2FA** vuelve a destacar con un aumento significativo (de 2.309 a 3.336 detecciones), retomando una tendencia claramente ascendente y reafirmándose como la amenaza predominante a nivel nacional, especialmente asociada a la evasión de controles de identidad y el compromiso de autenticación multifactor. En paralelo, **EvilProxy** mantiene su crecimiento sostenido y **AsyncRAT** muestra un aumento moderado, mientras que **DCRat** registra un incremento proporcional relevante pese a su menor volumen absoluto, lo que sugiere mayor actividad de campañas de acceso remoto en fases iniciales. Por el contrario, se observan descensos en familias previamente destacadas como **Sneaky 2FA, XWorm, Mamba 2FA** y Remcos, lo que apunta a una posible rotación táctica o a la priorización de infraestructuras de phishing más efectivas durante la semana analizada. En conjunto, el comportamiento refuerza un escenario dinámico, con énfasis renovado en plataformas de phishing avanzado y malware orientado al acceso persistente.

Más Información

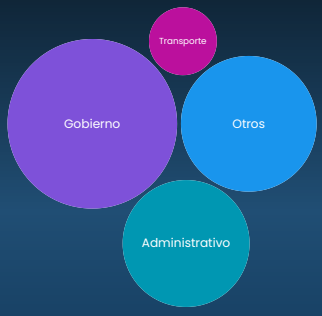
El mundo

60
Ciber incidentes

TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS

Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co